1. What is phishing?

Answer:
Phishing is a type of cyberattack where attackers trick users into revealing sensitive information such as login credentials, credit card numbers, or personal details by impersonating a trusted entity through fake emails, websites, or messages.

---

2. How to identify a phishing email?

Answer:
Phishing emails often include:

- Spoofed sender addresses
- Urgent or threatening language
- Suspicious links or attachments
- Generic greetings like “Dear User”
- Poor grammar or spelling errors
- Requests for personal or financial information

---

3. What is email spoofing?

Answer:
Email spoofing is the act of forging the sender’s address to make an email appear as if it's coming from a trusted source, even though it actually originates from an attacker-controlled server.

---

4. Why are phishing emails dangerous?

Answer:
Phishing emails can:

- Steal personal and financial information
- Spread malware or ransomware
- Lead to identity theft
- Compromise company systems and data

---

5. How can you verify the sender’s authenticity?

Answer:
You can verify a sender by:

- Checking the full email address, not just the display name
- Using domain verification tools (e.g., SPF, DKIM, DMARC checks)
- Contacting the sender through official channels
- Checking the email header for mismatches

---

6. What tools can analyze email headers?

Answer:

- **MxToolbox** – https://mxtoolbox.com/EmailHeaders.aspx
- **Google Admin Toolbox**
- **Header Analyzer by Microsoft or Cisco**

---

7. What actions should be taken on suspected phishing emails?

Answer:

- **Do not click** any links or download attachments
- **Report** the email to your IT or security team
- **Mark** it as phishing/spam in your email client
- **Delete** the email from inbox and trash
- **Update** passwords if you've clicked any links

---

8. How do attackers use social engineering in phishing?

Answer:
Attackers use social engineering to manipulate emotions such as fear, urgency, trust, or curiosity to make the user act quickly without thinking — like clicking a malicious link or sharing personal details.